WHAT IS CLAIMED IS:

1. A digital information security system comprising:

a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal;

a data storage unit for storing user information and digital information; and

a user management tool installed in a server, the user management tool being structured to receive the unique user key created by the user application tool, the user management tool being structured to store the received unique user key in the data storage unit, the user management tool being structured to compare the stored unique user key with a unique user key provided from the user application tool of a user currently being subjected to authentication.

2. The digital information security system as claimed in claim 1, further comprising a history manager for managing user access and use history.

3. The digital information security system as claimed in claim 1, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal.

4. The digital information security system as claimed in claim 1, further comprising a rule establishing unit for establishing a established rule according to a user rule previously established for the stored digital information, wherein the user application tool transmits information on the user rule during download of the digital information to the user, wherein upon downloading the digital information, the user application tool determines whether to output the downloaded digital information according to the established rule.

5. The digital information security system as claimed in claim 4, wherein said digital information includes an encrypted user requested digital file and a digital file decoding key using said unique user key and said rule information.

6. A digital information security method comprising:

reading a first unique user key created using unique system information

of a user terminal when a sever is accessed by a user;

comparing the first unique user key with a second unique user key included in previously stored user information for the user, to authenticate whether the user is an authorized user;

encrypting a file uploaded by the authorized user using a preset encryption key, and storing the encrypted file as digital information; and

encrypting a decoding key for the corresponding digital information using the second unique user key included in the user information, and downloading the encrypted decoding key along with the associated digital information in response to a digital information download request of the authorized user.

7. The digital information security method as claimed in claim 6, further comprising the step of decoding the digital information by decoding the encrypted decoding key for the digital information downloaded from the user terminal using the first unique user key created from the unique system information,

8. The digital information security method as claimed in claim 6, wherein the downloading includes said encrypted digital file and said decoding key of said encrypted digital file and rule information on use authority.

9. The digital information security method as claimed in claim 6, further comprising:

transmitting to the user a program for creating and transmitting the first unique user key using the unique system information of the user terminal when the user is unregistered, so as to allow the user to install the program in the user terminal; and

registering by the installed program the corresponding user using the first unique user key.

10. A digital information security method comprising the steps of:

creating a unique user key at a user terminal using unique system information of the user terminal;

decoding an encrypted decoding key included in the digital information at the user terminal using the created unique user key; and

decoding the digital information using the decoded decoding key, wherein the encrypted decoding key cannot be decoded when the key used for

decoding the encrypted decoding key is not identical to the created unique user key.

11. A digital information security system comprising:

a key management service module installed in a user system, the key management service module being structured to encrypt user information including a unique user ID created based on system information of a corresponding user from a user application tool installed in a system of the user, and storing the encrypted user information;

a document management service gateway structured to create a document key for the file when a file is uploaded from the user store the created document key, and encryp a corresponding file using the created document key;

a document distribution service module structured to create an encrypted download file including information on an output rule of the file in a predetermined user environment when downloading the file to the user; and

a web server structured to transmit information on the file uploaded through the Internet by the user to the document management service gateway so that the document management service gateway encrypts the file, and transmitt, upon receipt of a file download request from the user, information on the request to the document distribution service module so that the document distribution service module creates an encrypted download file for the file.

12. The digital information security system as claimed in claim 11, wherein the user application tool is structured to create the unique user ID and transmit the user information during initial installation and upgrade of the user system.

13. The digital information security system as claimed in claim 11, wherein the user application tool includes a document viewer module structured to call a plurality of document edition software programs, output the called programs in a predetermined window, and allow the user to execute the document edition software programs.

14. The digital information security system as claimed in claim 13, wherein the document viewer module is structured to allow the user to execute the document edition software program on the window, and determine whether to perform a predetermined execution control operation including an operation of saving and printing a predetermined file according to predetermined rule

information and user information for the file downloaded during execution of the document edition software program.

15. The digital information security system as claimed in claim 11, wherein communication among the document key management service module, the document management service gate, the document distribution service module and the web server is performed through TCP/IP (Transmission Control Protocol/Internet Protocol).

16. A digital information security method in a digital information security system including a documents key management service module for managing user information including a unique user ID created based on system information of a user, a document management service gateway for encrypting a corresponding file by creating a document key for an uploaded file, a document distribution service module for creating an encrypted download file including information on an output rule of a file to be downloaded, and a web server for performing a file uploading/download operation with the user through the Internet, transmitting information on an uploaded file to the document management service gateway and transmitting information on a download request to the document distribution service module, the method comprising the steps of:

transmitting by the web server information on the uploaded file to the document management service gateway;

reading by the document management service gateway the uploaded file by accessing a position where the file is actually uploaded from the server, using the information on the uploaded file;

creating a document key for the read file in a predetermined decoding method, and storing the created document key along with the corresponding file information;

encrypting the file using the created document key;

storing the encrypted file in a predetermined folder; and

informing the web server that processing the uploaded file is completed.

17. The digital information security method as claimed in claim 16, further comprising the steps of:

upon receipt of a file download request, transmitting by the web server information on a download-requested file to the document distribution service module;

accessing by the document distribution service module a corresponding encrypted file using the information on the download-requested file;

creating an encrypted download document file matched with an authority of the user based on user information of the user and information on the document key for the document and the output rule;

storing the created encrypted download file in a download position; and

informing the web server that processing the download-requested file is completed.

18. The digital information security method as claimed in claim 16, wherein the information on the output rule includes a save authority which is a rule indicating whether the user can save the download document file in a user terminal of the user, a print authority which is a rule indicating possibility and number of printing the download document file, an available term authority indicating a rule for an available term of the download document file, and an assignment authority indicating a rule for assignment of the download document file.

19. The digital information security method as claimed in claimed 17, said creating an encrypted download document file includes combining said rule information on said authority with said decoding key of said encrypted file and encrypting said rule information and said decoding key using said unique user ID and combining combined said rule information and decoding key with said encrypted download document file.